AFRL-IF-RS-TR-2006-8
Final Technical Report
January 2006

ANALYSIS OF ACTIVE RESPONSE IN THE IMMUNE SYSTEM WITH COMPUTER NETWORK CONSIDERATIONS

Victor A. Skormin

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2006-8 has been reviewed and is approved for publication

APPROVED: /s/

JOSEPH J. GIORDANO
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, JR., Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
JANUARY 2006

3. REPORT TYPE AND DATES COVERED
Final Jan 05 – Jul 05

4. TITLE AND SUBTITLE
ANALYSIS OF ACTIVE RESPONSE IN THE IMMUNE SYSTEM WITH COMPUTER NETWORK CONSIDERATIONS

5. FUNDING NUMBERS
C - FA8750-04-1-0189
PE - N/A
PR - 558B
TA - II
WU - RS

6. AUTHOR(S)
Victor A. Skormin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Victor A. Skormin
352 Ford Hill Road
Berkshire New York 13736

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/IFGB
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2006-8

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Joseph J. Giordano/IFGB/(315) 330-1518/ Joseph.Giordano@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 Words)*
Response of the immune system to invading alien proteins is considered as an example of a highly successful defense mechanism of a complex system against an, effectively, information attack. Specific components of this mechanism are described and subjected to mathematical modeling. The entire mechanism is viewed as a closed-loop, nonlinear, negative feedback circuit. Generic conditions resulting in two distinctive outcomes of such an attack, lethality and full recovery are established. The control law, inevitably resulting in the full recovery outcome is described. A chronology of a recent information attack on the international computer network community is presented, and the resemblance between the particular stages of the attacks on the computer network and the immune system is emphasized. It is concluded that the control law established for the immune defenses could be fruitful in application to computer defenses.

14. SUBJECT TERMS
Immune System, Lethality

15. NUMBER OF PAGES
17

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

List of Figures

1. Introduction

Modern immunology provides a detailed but rather qualitative description of the active response of the immune system to any entity invading the organism and recognized as an antigen by the immune cells. In a similar way that a malicious computer program is constructed from the same instructions as legitimate software but sequenced in a fashion that makes it malicious, an antigen is constructed from the same building blocks as the cells of the host but differently sequenced. In many ways, the effects of an antigen on a biological organism are similar to those caused by some information attacks on computer networks. This is the major reason for considering the active response of the immune system, honed to perfection by million-year evolution, as an ideal mechanism for protecting computer networks from information attacks.

The specific immune response is the main mechanism enabling the immune system to destroy cells of the intruding antigen. The outcome of this process (recovery, chronic infection or lethality) greatly depends on the time between the infection and detection of the antigen, and growth rates of the antigen cells and immune cells competing for the limited resources of the host. After the antigen has been defeated, the residual concentration of specialized fighter cells slowly decreases providing high immunity to similar infection. We attempt to describe the active response mechanism of the immune system in terms of a negative-feedback closed-loop system and establish nonlinear differential equations of its particular components thus resulting in a mathematical model of the immune response. Subjected to analytical techniques offered by modern control theory, this model will enable us to establish the conditions for three possible outcomes of such interaction, full recovery, chronic infection, and lethality, and to formulate a control law assuring the full recovery outcome.

We will demonstrate that an equivalent of every stage of the immune response could be observed in our experience with computer epidemics. Consequently, the model of the immune response, describing the principle of operation of a successful defense mechanism against information attacks, has great potential for the analysis and synthesis of defenses for a computer network. The control law synthesized using the methodology of advanced control theory to assure a full recovery outcome for the immune system can be reformulated in terms of the characteristics of computer networks and interpreted as a set of instructions to a network manager.

While computer networks became one of the critical and increasingly vulnerable components of the national infrastructure, our research addresses this reality presenting a methodology for the analysis and synthesis of the information security systems for computer networks that emulates the genetically optimized mechanism of active immune response. It is said that the immune response is genetically optimized for its biological environment; although this is different from a computer network, this difference narrows with every recent advancement in nano-technology and synthetic protein-type computing media that will result in large-scale integrated computer networks whose operation will resemble the living tissue. The presented effort presents an innovative approach to mathematical modeling, computer simulation, analysis, design and control of complex systems resulting from these emerging technologies, and provides the visualization and important insight into the interrelation of physical phenomena behind their operation.

This work is a logical continuation of the research conducted by the authors under the Air Force funding. In 2001 they engaged in the project BASIS (Biological Approach to System Information Security) aimed at the analysis of the aspects of the specific immune response that have the potential for the implementation in the new generation of computer network security systems [1, 2, 3]. This project has resulted in the "engineering view" of the immune mechanisms and prompted several new concepts in computer security. First, utilizing the modern findings of immunology the concepts such as formal protein and formal immune network were formulated presenting a novel approach to modeling the immune system. The capability of the immune system to make a distinction between the "self" from "non-self" with high degree of dependability by determining the binding energy between proteins was emulated using the methodology developed in matrix analysis. The computational approach involving the concept of binding energy was proposed as *Immunocomputing* for the implementation in novel computing media and application for the solution of a wide class of computationally intensive problems [4].

The second BASIS-inspired concept was the detection of malicious codes by detecting its "gene of self-replication". Indeed, a high percentage of information attacks are perpetrated by deploying computer viruses and worms, which result in very costly and destructive "epidemics". Spread of malicious codes is achieved by the built-in ability to self-replicate through the Internet and computer media. Since most legitimate codes do not self-replicate, and the number of ways to achieve self-replication is limited to the order of fifty, the detection of malicious codes could be reduced to the detection of the "gene of self-replication" in the code in question. This research effort is on the way and, according to current results, is highly successful [5].

2. Anatomy of the active immune response

The specific immune response is the main mechanism enabling the immune system to destroy cells of the intruding antigen. This is accomplished by multiplying, on demand, fighter cells that are uniquely equipped for counteracting this particular antigen by carrying its genetic sample. The immune system is prepared to counteract practically any antigen as it contains cells that specialize in at least 10^{15} various genotypes. However, the actual ability of the immune system to destroy an intruder depends on its ability to generate specialized fighter cells at the necessary rate, i.e. to actively respond to the intruder.

Active response of the immune system includes several stages. It starts from the intrusion of the antigen cells in the biological organism. Intruding cells quickly multiply and their concentration exponentially increases thus increases the probability of a physical contact of an antigen cell with a specialized immune cell capable of recognizing it as an antigen. The initial concentration of these specialized cells depends on the previous exposures of the organism to this antigen (i.e. acquired immunity). The detection of the antigen triggers the process of exponential proliferation of immune cell-fighters specialized to destroy the antigen cells. Multiplying antigen cells and multiplying immune fighter cells compete for limited resources of the biological organism. It could be seen that the outcome of this process (recovery, chronic infection or lethality) greatly depends on the time period between the moment of infection and the moment of detection of the antigen. When the proliferation of the antigen cells goes too long before detection, its cells consume a greater share of the resources of the host thus preventing the fighter cells from sufficiently multiplying, leading to lethality. A high initial concentration of specialized fighter cells (after the organism has been immunized for a particular infection) facilitates early detection of the antigen and prevents it from overwhelming the immune defenses. After the antigen has been defeated, the residual concentration of specialized fighter cells slowly decreases providing high immunity to similar infection. It could be seen that at certain conditions, parity between proliferating antigen and fighter cell could be achieved leading to chronic infection.

3. Mathematical model of the immune response

The mathematical model of immune response reflects the basic concepts and phenomena of immunology and describes the dynamics of the immune process at the organism level. The individual components of a living organism's immune response are not essential to the analysis of the dynamics of the response to an antigen attack, therefore only the basic mechanisms of the protective reaction of an organism without distinction between cellular and gumoral responses will be reflected. Included in the generalized definition of protective cells are the components of cellular/lymphoid systems as well as the gumoral/immunoglobulin system. This includes leukocytes, lymphocytes, antibodies/immunoglobulin and cellular structures that are capable of neutralizing a given antigen. Antigen is defined as any organism or material alien to a targeted system that is capable of causing an immune response. Based upon these preliminary assumptions the mathematical model of the immune response presents a combination of the following components.

Limited resources of the organism: Proliferation of the antigen cells as well as the immune cells in a living organism is possible only if there are available resources. Antigen and immune cells compete for these resources while consuming them. These resources are being restored by various processes within the organism and are maintained at some level that slow decreases due to ageing. Mathematical model of the immune response will include a non-negative variable providing a quantitative representation of the vital resources of an organism. A single-loop control mechanism responsible for maintaining the level of resources and special parameters regulating the rate of ageing will be introduced in the model.

Initial concentration of specialized immune cells: The concentration of the specialized immune cells prior to attack will be emulated by a constant, in the case of "normal" low immunity, or slow decreasing exponential, in the case of high immunity acquired after previous infection by the same antigen.

Proliferation of the antigen cells: The initial concentration of the antigen cells will be represented by some amount in the moment of infection representing the severity of infection. Antigen concentration dynamics after the moment of infection corresponds to models of population growth. One of the elementary models of a population growth was introduced by T. Maltus based upon the tendency of a population to increase in a geometrical progression. In nature, many life forms are capable of propagating in a geometrical progression, however, factors such as competition for resources, disease, and death (natural and forced) present obstacles for the sustaining growth. Ferhulst first introduced the mathematical form of an S-shaped growth curve also referred to as the Ferhulst logistical curve. The inclinations of S-curve grow exponentially in the beginning then gradually flatten towards zero. At large time values the curve converges to a horizontal line represented by which describes the equilibrium value of a population size.

The equation, which describes the rate of change in concentration of an antigen after the moment of infection, could be developed using one of the equations of natural dynamics [10]. In the case of antigen introduction, a cascade increase in the concentration of antigen takes place due to absorption of vital resources of the host. In the beginning, the amount of available resources does not influence the rate of increase of antigen until the concentration of the antigen exceeds some threshold. Upon reaching this level, the resources of the host organism will not be sufficient to sustain the cascade growth of the antigen, therefore, the growth rate of the antigen will gradually decrease to a minimum level. The given process can be described by a nonlinear logic function that reflects only the presence or absence of resources sustaining the increase of the antigen concentration.

Detection of the antigen: Detection of the antigen is the event visualized as the first physical contact of the antigen cell and the specialized immune cell "equipped" to recognize this antigen. It could be seen that the probability of this event increases with the increase of the concentrations of both the antigen cells and the specialized immune cells. Prior to the moment of infection, the concentration of the specialized immune cells could be viewed is a slow decreasing exponential function, practically a constant. It is the multiplication of the antigen cells that causes the increase of the probability of the antigen detection with time making this event inevitable over some period of time. One could assume that the *detection time* can be defined as the time period during which the probability of detection reaches some sufficiently high value. It could be seen that in the case of elevated immunity of the organism, i.e. high initial concentration of the specialized immune cells after previous attack by the same antigen, the detection time is shorter then in the case when the organism has never been exposed to the antigen. Shorter detection time also causes immune defenses to be activated at an earlier stage of the antigen multiplication process that significantly increases the chances of the multiplying immune cells to successfully compete for the limited resources of the organism.

Interaction between the antigen and immune sells: From the point of infection, antigen cells are destroyed by the specialized immune cells that results in the reduction of the antigen cell concentration. Consequently, the differential equation of the concentration of the antigen cells would reflect the following phenomena,

a) Multiplication of the antigen cells affected by the available resources of the organism;

b) Resources of the organism affected by the proliferating antigen and immune cells;

c) Neutralization of the antigen cells by immune cells dependent on the concentrations of both cells, the probability of a binding between an antigen and an immune cells, and a number of immune cells participating in the neutralization of one antigen cell [11];

The probability of a binding also depends on the concentrations of the antigen and immune cells and the resources of the organism [12].

Dynamics of the concentration of the immune cells: The concentration increase of the immune cells is triggered by the detection of the antigen and takes place only when there is a surplus of resources. The rate of increase is also dependent on the availability of resources. This reality is well known in immunology: low initial immunity level resulting in long detection time and/or large amount of the antigen introduced at the moment of infection allow the antigen cells to consume a large share of the resources of the host thus preventing the immune cells from proliferating at the necessary rate.

When developing the equation that describes the dynamics of concentration of the immune cells in the presence of antigen, it is necessary to take into account that the organism concentrates its response primarily in the region where most of the antigen cells are located. With a small antigen concentration, there is a weak stimulation of lymphocytes. If the antigen concentration is large, many lymphocytes may reach the end of their ability to propagate [12].

The differential equation of the concentration of the immune cells reflect,

a) The cascade growth of the concentration of immune cells binding with an antigen stimulated by the presence of an antigen;

b) The decrease of the concentration of immune cells as a result of interaction with antigen;

c) The dynamics of the available resource of the organism

Finally, *the mathematical model of the immune response system* can be defined as a system of nonlinear differential equations interrelating three time-dependent *variables* that represent

a) Vital resources of the host organism,

b) Concentration of the antigen cells

c) Concentration of the specialized immune cells

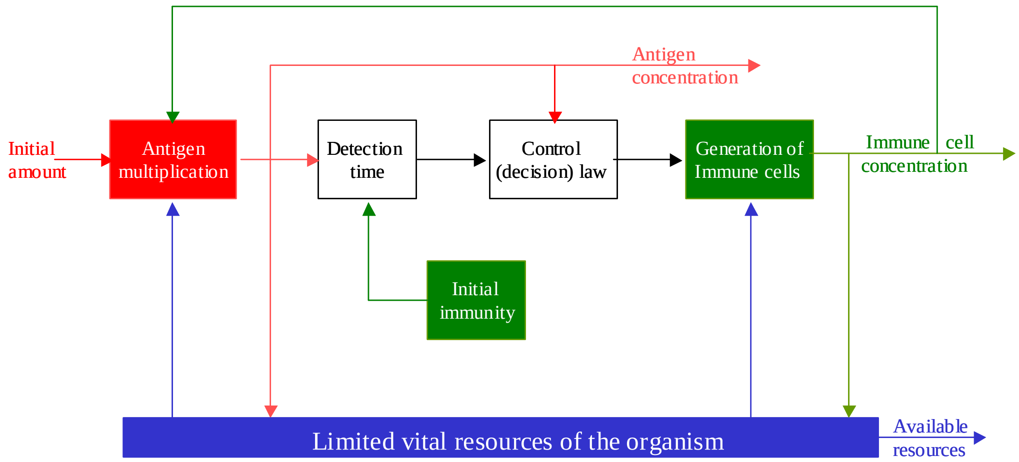

Figure 1. Simulation model of the immune response

The incomplete list of *parameters and constants* of the mathematical model includes

- rate of natural ageing of the organism (resource reduction)
- coefficients of an organism’s recovery rate
- amount of resources of the organism per unit of antigen cell concentration
- amount of resources of the organism per unit per unit of immune cell concentration
- rate of cascade growth of the antigen concentration due to availability of resources
- rate of the concentration change of the antigen due to unavailability of resources
- reduction of the antigen concentration due to the interaction with immune cells
- rate of growth of the immune cell concentration under the availability of resources
- rate of decrease of the immune cell concentration when resources are unavailable
- reduction of the immune cells concentration due to the interaction with the antigen

A preliminary version of such a model established under the Air Force funding [1] and implemented in simulation environment providing the means for the quantified visualization of particular components of the immune response. It is understood that the model is lacking some details and the choice of its parameters is not fully supported by literature. Nevertheless, the model allows for simulation analysis of the conditions leading to three possible outcomes of the antigen attack on the living organism.

4. Outcomes of the immune response

The immune response is modeled as a continuous dynamic process [1]. The biological variability or casual statistical fluctuations was disregarded thus the model represented average values of the appropriate variables. The qualitative side of the particular phenomena was reflected by the choice of coefficients (gains).

4.1 Primary and secondary immune response with the full recovery outcome

This outcome results in the elimination of the entire population of the antigen cells and is expected when the organism's resources are sufficient for supporting the necessary rate of multiplication of the immune cells. After the initial infection, the antigen cells multiply undetected by the immune system. This period is referred to as the incubation period of the disease. The length of this period can vary as antigen may lie dormant waiting for some “trigger event” to awaken it. Once detected, there is an additional period of time during which the immune cells and antigen multiply without significant interaction: at the beginning stages of the antigen attack the immune system concentrates its efforts on creating appropriate cells to respond to the newly discovered infection. When the concentration of antigen reaches some level, the second phase of the immune response, the growth phase, begins with the occurrence of the antibodies in the blood whose concentration increases over a several day period to the highest possible level. This is the most active phase of the immune response to an antigen. At this phase, the concentration of antigen cells begins to decrease as a result of the annihilating by immune cells. In addition, the growth of the concentration of immune cells slows the rate of multiplication of the antigen cells that ultimately results in the elimination of antigen.

After the population of antigen is nearly suppressed, the final phase of the immune response begins. This phase is referred to as the attenuation of the immune response. It ends with the residual level of specialized immune cells being much higher that prior to the antigen attack resulting in the high (acquired) immunity of the organism to this particular antigen.

During all three phases of the primary immune response, populations of antigen and protective cells are consuming resources of the organism causing their level to decrease, especially during the period of the greatest concentration of antigen and immune cells. It important that the resource level does not become the factor limiting the multiplication rate of the immune cells that becomes the condition for the full recovery outcome.

The secondary immune response occurs with a repeated infection of an organism by the same antigen. Then due to high initial concentration of the specialized immune cells (high immunity) the antigen is detected virtually immediately and all stages of the immune response take place very fast with very little impact on the resources of the organism.

The simulation analysis results illustrating the full recovery outcome of the immune response are shown below.

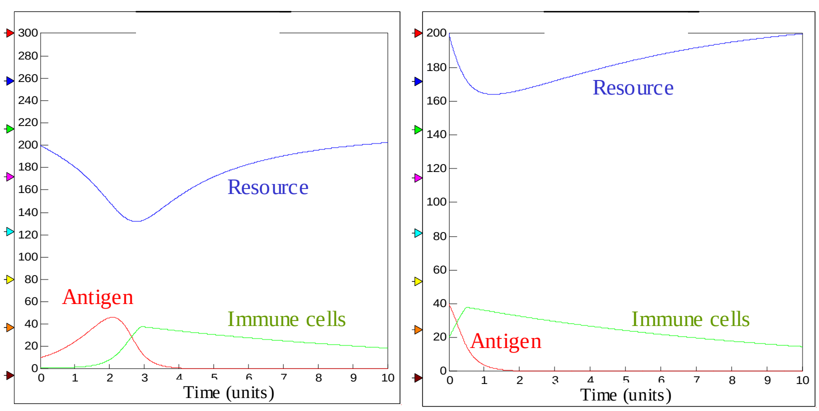

Figure 2. Primary and secondary immune responses with full recovery

4.2. Failure of the immune response: lethality or chronic illness

A severe infection in combination with low initial immunity and insufficient immune response results in lethality or chronic illness. This case exhibits very late immune response or aggressive growth of antigen leading to high antigen concentration consuming most of the resources of the organism thus causing significant pathological changes in an organism and consequent failure to sustain or intensify the immune response. In either case, the multiplication rate of the specialized immune cells becomes insufficient for the suppression of antigen.

The simulation study conducted on the preliminary model of the immune response [1] facilitates convincing visualization of the complex phenomena of the immune response (see below). It could be seen that in the first case the lethality is caused by a high volume of the antigen introduced in the organism, and in the second case by low resource level of the organism in combination with low initial immunity. It should be noted that the moment of death is recognized as the instance when the resource level of the organism becomes equal to zero. Note the graduate decline of the antigen after the death of the host.

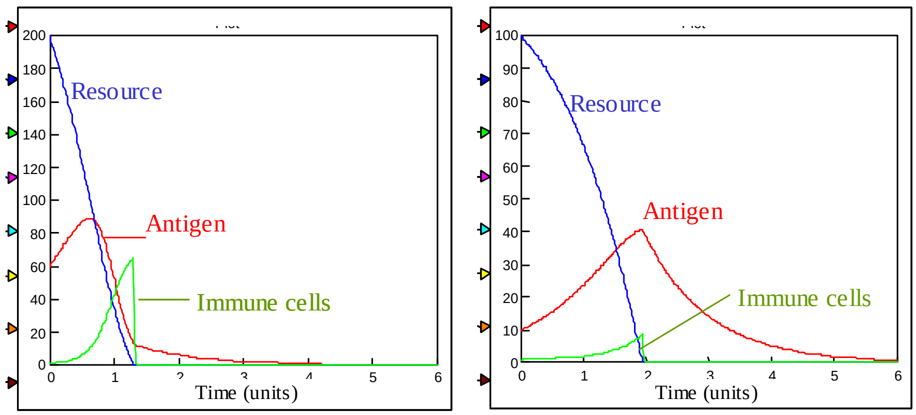

Figure 3. Immune responses resulting in lethality

The chronic illness outcome of an immune response could be also easily modeled and visualized using the existing model as a situation when the rate of multiplication of the antigen and immune cells and the restoration of the resources of the organism reach equilibrium. This situation is well known in immunology and medicine.

It should be emphasized that three major components of the immune response, the antigen growth, the growth of the immune cells, and the dynamics of the organism resources for an obvious closed-loop chain of transformations that constitutes a highly nonlinear, time-dependent, multivariable negative feedback system that *does confirm* to advanced analysis and synthesis theory developed in modern controls.

The refinement of the presented model and detailed analysis of specific situations known in modern immunology are being conducted. However, the described model cannot be fully exploited in immunology. It is difficult to assign values to the various parameters and to adjust the responses. Many of the parameters are locked in the complexity of the immune system and parameters are simple fundamentals of nature. In a system of computer networks, at any scale, each parameter can be estimated. Simulations would provide network planners with an accurate estimate on how to harden networks and services. Furthermore, unlike a biological system, the response can be tuned to provide the desired outcome.

5. Control of the immune response

The resultant mathematical model of the immune response facilitates the understanding and numerical simulation of major interactions between the components of the immune system and the intruding antigen. Subjected to analytical techniques offered by modern control theory and numerical analysis, this model enables us to establish the conditions for three possible outcomes of such interaction, full recovery, chronic infection, and lethality, and to formulate a control law "enforcing" the full recovery outcome. The control law developed for the closed-loop system represented by the model is visualized as a mechanism capable of modifying the properties of the underlying biological phenomena in order to assure the full recovery outcome. It could be seen that the full recovery outcome can be assured by

- high intial immunity (i.e. the enhanced ability to detect the intruding antigen),

- high rate of multiplication of the specialized immune cells, and
- maintaining the resource level of the organism necessary to sustain the high rate of multiplication of the immune sells. Since these characteristics are defined by the appropriate numerical values of the parameters of the mathematical model, the control law could be expressed by the definition of the respective model parameters as functions of the current level of the antigen concentration. Unfortunately, this control law implies the modification of major biological mechanisms and as such cannot be recommended to a physician and can be applied only to the simulation model of the immune response.

However, the main value of this model justifying the effort of its development is that it provides a description of a highly successful active response of a complex system utilizing a very large number of semi-autonomous agents. Consequently, describing defenses of a computer network against information attack in terms of this model provides the means for the analysis of this complex process and allows for the adoption of the established control law leading to the only desirable outcome, the full recovery. Unlike the immune system, characteristics of a man-made computer network are very likely to be adequately represented by the model parameters.

6. Anatomy of an information attack on a computer network - a recent example

The following chronology of events, describing one of the recent internationally known information attacks, is presented to emphasize its similarity to the chain of events observed in the immune system defending the biological organism against antigen.

In August and September of 2003, the W32/Blaster worm and its variants targeted computer systems running various Microsoft Windows operating systems. Before the onslaught, there came plenty of warnings with recommended actions for system administrators and computer owners to prevent potential infection from a yet unknown (and non-existent) assailant. On July 16, 2003, Microsoft released a security bulletin (MS03-026) with a *critical* severity rating and a software patch to update affected systems. According to Microsoft, the security hole would allow a remote potential assailant to "run code of attacker's choice."

On July 17, 2003, many news outlets covered the newly discovered vulnerability as the first discovered flaw in the Windows Server 2003 platform and indicated that previous versions of the operating system were also affected. Microsoft indicated that this security hole would allow for hackers to seize control of the target computer, steal data, damage files, or potentially eavesdrop on communications [Fox News July 17, http://www.foxnews.com/story/0,2933,92212,00.html -- "Microsoft Admits Flaw in Windows Software"]. People running the installed operating systems were urged to install the software patch to correct the problem.

August 11, 2003 was when the first attack from the W32/Blaster worm was detected. CERT, a well established center for reporting software vulnerabilities and virus/worm related incidents, issued advisory CA-2003-20 detailing the discovery, but offered little advice on how to eliminate infection or prevent infection on non-patched systems. Headlines followed with Fox News reporting "Internet Attack Disables Thousands of Computers" on August 13 and the Department of Homeland Security issuing an Internet worm advisory on August 14 [http://www.dhs.gov/interweb/assetlibrary/Blaster_Worm_Advisory.PDF]. Within three days of the initial detection, the major anti-virus companies issued updates to their virus detection software to detect Blaster, CERT, Microsoft, and the Department of Homeland Security had listed methods and techniques to prevent infection or to repair a compromised system, and over 188,000 computer systems worldwide were infected [Network World Fusion http://www.nwfusion.com/news/2003/0812blastinfect.html -- "Update: Blaster worm infections spreading rapidly"]. Even though the vulnerability was known for approximately a month before the actual infection, severe damage occurred. High profile users, such as the Maryland Department of Motor Vehicles and the U.S. State Department, were among its victims. Soon after the release of Blaster, the mutants, using similar means for infection, began to propagate.

The Blaster worm infects a host by exploiting a buffer overrun in Microsoft’s DCOM RPC service. A carefully crafted packet is sent to a host using TCP port 139. This packet results in a buffer overflow that causes code transferred through this connection to begin executing. Upon execution, a copy of Blaster is obtained from the infecting host and is installed on the newly infected machine. At this point, the infected host executes Blaster and begins to infect other hosts using the same technique. Part of the payload of the worm is a TCP SYN flood against the very servers at Microsoft that distribute the needed software patch to permanently immunize a system from Blaster.

Before the assault, except for the systems that had received the corrective patch or were behind properly configured firewalls or were naturally immune to Blaster, there was no mechanism to detect an attempt to infect any given target machine. Detection of the attack only occurred after infection by the computer operator and only after the new host machine spread the infection to a number of other hosts. In other words, the initial concentration of immune detectors was quite small. As more machines became infected, the concentration of antigen increased. This continued until computer operators noticed unusual activity, reported it and the response began. This is referred to as the threshold of detection.

As Blaster spread, available resources were consumed. Ultimately, these resources were uninfected vulnerable hosts, bandwidth to the Microsoft update servers, bandwidth of compromised machines and the number of operators available to respond to the infected machines. Furthermore, already infected machines became victims of Denial of Service (DoS) attacks caused by future attempts to infect. These machines typically stopped responding or forcibly reboot.

The response began with organizations releasing information about the new worm and methods to prevent infection. Antivirus manufacturers released updates to their definition files that would detect and stop Blaster from infecting a vulnerable host or prevent a host from infecting future machines, however, the “protected” machine would still hang or reboot after an unsuccessful attempt at infection, preventing further legitimate use of the system. The installation of the updated definition files ultimately rested in a valid subscription to the definition files or a specific action on behalf of a computer operator. Furthermore, Microsoft released information on how to prevent infection of an un-patched host. The consequence of the prevention measures was that some heavily used remote services would become crippled.

With each newly developed or implemented defense technique, the effective concentration of fighter cells increased. The cost of the response included both manpower and bandwidth. Each infected machine required an operator to physically recover it. The recovery process involved obtaining the patch from Microsoft, requiring bandwidth, and a period of time where the machine, while obtaining and installing the patch didn’t malfunction as a result of another attack.

Within a few weeks of the first infection, hundreds of thousands of machines were affected. The response took several days, during which mutants of Blaster began circulating. Many machines became permanently immune during this period, with the proper software patches installed. However, many machines existed in “safe” environments, out of the reach of Blaster, until some event in the future re-exposes them to risk. As an example, one of the responses to the worm was to firewall off the network services that Blaster exploited. It can be realized that these are only temporary, and in the future, the firewall protection can be eliminated. This slow denigration of defenses is one of the components of the natural aging of the computer network.

The primary reason that Blaster was able to perform as much damage as it did is a direct result of a long delay period between the initial infection and the response. A large number of machines became infected consuming a large quantity of resources that could have otherwise gone into fighting off the worm. This results from a primarily *human* detection mechanism and a *human* protection mechanism. After all, if all of the systems were inoculated (with the software patch), there would not have been an infection. Or, if an alternative mechanism could have challenged the initial infection similar to ones proposed in [5] and [8], this delay period could have been seriously reduced.

7. The computer network considerations

The parameters obtained for the model of the immune system can be extended to computer systems and networks of computer systems to model the effects of various attack mechanisms. The prime difference, however, between a computer network and a living organism is that each of these parameters needs to be established for a particular attack mechanism and a specific service or group of services. The mechanisms of immune responses described by the immune model are relatively uniform, with many of the same cellular groups performing common functions. Furthermore, resource availability is relatively uniform for any given attacker and any given response. For consistency, extension of a biological immune response model to a specific information attack on a computer network will require a specific set of parameters.

The level of available resources within a computer network can be comprised of many different elements and referred to as the *throughput* of the computer network. This is an aggregate parameter, composed of at least one and potentially many parameters. Within a computer network, there are a number of components that can be consumed by both that attacker and the response mechanism. Examples of these components are processing capability of the various networking components, bandwidth, queue depths, machine and process throughput and latency, etc.

A simple example is a TCP/IP SYN flood attack, which is a form of denial of service (DoS) attack. The point of the assault is to render the server attached to the network *offline*. This is accomplished by filling the half-open TCP connection queue with phony connection requests. The important components of the network resources are the TCP connection queue depth and CPU time required to analyze each connection to verify authenticity of the host attempting the connection. A more complicated example is an Internet worm, the likes of Code Red or W32.Blaster, which, through their replication and subsequent infection disable host after host. In this case, the required resources is composed of valid “uninfected” hosts, human resources available to apply the appropriate patches, network throughput for the spread of infection, and time to apply the appropriate fix before the host computer is disabled.

The relative concentration of *detector cells and responders* for the attack mechanism can be represented by the ratio of computer operators to the number of machines on a network with properly configured and updated anti-virus software to a complex mechanism analyzing every packet exchanged on a network. As in the biological immune system, many of the detection mechanisms in the computing world are forms of signature detection. As in a biological system, the detectors are free to roam and detection occurs when the detector happens upon an antigen, to reduce overhead, network packets may be sampled or only checked against a specific signature and allowed to pass. In this case, the detector concentration can simply be the number of signatures within a large set applied to each packet at a specific checkpoint.

The *concentration of the antigen* represents, in computer terms, the frequency or depth of the attack. As in the biological immune system, this is an attack specific parameter. This can be the number of machines infected with a computer virus, the number of half open TCP/IP SYN requests per second, level of bandwidth consumption by malicious activity, number of e-mail messages processed per second, etc.

In an immune system, there is a parameter that describes the threshold of detection, which represents the concentration of antigen at which detection occurs. This parameter is inversely proportional detector concentration. For example, if a virus or worm attacks and is previously unknown, at a minimum, it is simply related to the number of trained computer operators which directly observe the attack.

The coefficients of an organism's *recovery rate* represent the restoration of resources as a result of immune activity and due to normal recovery. There is no simple analog to this parameter in a computing network. This can be viewed as a complex interaction of computer administrators ensuring clean and well-protected systems along with properly sized and maintained network connections.

The *ageing of the immune memory* ultimately relates to the *human factor* of the network. At any given point in time, a computer system may be considered well protected, however, in the passage of time, various exploits in installed software are uncovered, holes in networking protocols are exposed and new viruses are developed. Unless the network is continuously undergoing updates, these weaknesses accumulate until some later event triggers an update. This phenomenon was demonstrated by the heavily publicized attack from the W32.Blaster worm. A patch, which repaired a previously discovered software deficiency, was available a month before the worm infected its first host.

During an attack and the subsequent immune response, the concentration of antigen undergoes cascade increase. Only after detection does the immune response begin. At this point systems administrators begin the first portion of the response, isolating infected machines, reinforcing existing defense mechanisms, isolation of *clean* networks to preserve integrity, installation of detection and repair software and infected systems recovery. Once mobilized, the response also undergoes cascade increase and continues until all affected systems are recovered and computer network systems performance is recovered.

It can be argued that in a computer network, ultimately, resources to repair and restore a network system are unlimited. Money and manpower are the prime resources and in the end will always succeed. Therefore, *death of the network* does not happen in the same sense as a biological organism. In a biological organism, when death occurs, it is final. In computing systems, true death is only the *permanent loss of information*. However, serious disruptions in computing services in high demand time-sensitive applications can and do cause loss of equipment, valuable resources and even human lives.

Knowing how to relate the parameters of a computer network to the biological immune system allow for modeling of various attack, detection of bottlenecks and assessment of vulnerabilities of the computer network. Furthermore, deficiencies in current network defenses can also be identified.

The control law established for the model of the immune response could be reformulated in terms of parameters of the computer network and implemented in automatic regime and/or through the actions of the network manager, providing a numerically justified basis for the reconfiguration of the network subjected to the information attack.

References

1. V. Skormin, “Biological Approach to System Information Security (BASIS): A New Paradigm in Autonomic Information Assurance”. Final Report to AFRL at Rome NY on Contract #30602-01-0509, Binghamton, NY, 2002

2. Skormin, V.A., Delgado-Frias, J.G., McGee, D.L., Giordano, J.V., Popyack, L.J., Gorodetski, V.I. and Tarakanov, A.O., BASIS: a biological approach to system information security, *Information Assurance in Computer Networks* (Gorodetsky V.I., Skormin V.A. and Popyack L.J. eds. LNCS 2052, Springer-Verlag, Berlin, 2001, pp. 127-142).

3. V. Skormin, D. Summerville, J. Moronski, D. McGee, "Biological Approach to System Information Security (BASIS): A Multi-agent Approach to Information Security", Lecture Notes in Computer Science, Volume 2691, Springer-Verlag Heidelberg, 2003

4. A. Tarakanov, V. Skormin, S. Sokolova, "Immunocomputing. Principles and Applications", 210 pp, Springer-NY, 2003

5. V. Skormin, D. Summerville, J. Moronski, “Detecting Malicious Codes by the presence of their *Gene of Self-Replication*”, “Computer Network Security”, Lecture Notes in Computer Science, Volume 2776, Springer, 2003

6. V. I. Gorodetski, I. V. Kotenko, L. J. Popyack, and V. A. Skormin, “Agent-Based Model of Information Security System: Architecture and Framework for Behavior Coordination”, *Proceedings of the First International Workshop of Central and Eastern Europe on Multi-agent Systems (CEEMAS'99)*, June 1999, pp. 323-331

7. V. Gorodetski, V. Skormin, L. Popyack (Eds.), "Information Assurance in Computer Networks. Methods, Models and Architectures for Network Security", Lecture Notes in Computer Science, Springer, 2001

8. V. Skormin, D. Summerville, J. Moronski, and J. Sidoran, “Application of Genetic Optimization and Statistical Analysis for Detecting Attacks on a Computer Network”, Proceedings of the Real-time Intrusion Detection NATO Symposium, May 27-29, Lisbon, Portugal, 2002.

9. V. Gorodetski, L. Popyack, V. Skormin (Eds.), “Computer Network Security”, Lecture Notes in Computer Science, Springer, 2003

10. T. Gard and J. Hoffacker, “Asymptotic Behavior of Natural Growth on Time Scales”, Dynamic Systems and Applications, Vol. 11, 2002

11. Anderson RW, Neumann AU, Perelson AS (Theoretical Biology and Biophysics, Los Alamos National Laboratory). A Cayley tree immune network model with antibody dynamics // Bull Math Biol 1993 Nov

12. Singer DF, Linderman JJ (Department of Chemical Engineering, University of Michigan, USA). The relationship between antigen concentration, antigen internalization, and antigenic complexes: modeling insights into antigen processing and presentation // J Cell Biol 1990 Jul.

13. Seiden PE, Celada F. (IBM T. J. Watson Research Center) A model for simulating cognate recognition and response in the immune system // J Theor Biol 1992 Oct .

14. Merrill S. Mathematical models of Humoral immune response // Techn. Rep. of the Univ. Of Iowa, 1976. – 40 p.

15. Batt BC, Kompala DS (Department of Chemical Engineering, University of Colorado). Verification of immune response optimality through cybernetic modeling // - J Theor Biol 1990 Feb.

16. Singer DF, Linderman JJ (Department of Chemical Engineering, University of Michigan, USA). The relationship between antigen concentration, antigen internalization, and antigenic complexes: modeling insights into antigen processing and presentation // J Cell Biol 1990 Jul.

17. Weinand RG, Conrad M (Department of Computer Science, Wayne State University, Detroit, Michigan). Maturation of the immune response: a computational model // J Theor Biol 1988 Aug 22

18. Morel PA (University of Pittsburgh). Mathematical modeling of immunological reactions // Front Biosci 1998 Mar

19. Mohler R., Barton C. Compartmental control model of the immune process: Proceedings of the 8th IFIP Conference on Optimization Techniques. – Heidelberg: Springer-Varlag, 1978.

20. Mohler R. Bilinear control structures in immunology // Proc. Of IFIP Worcing Conference on Modelling and Optimization of Complex systems. – Berlin a.o.: Springer-Varlag, 1979.

21. Mohler R., Barton C., Hsu C. System theoretic control in immunology. – Oregon State Univ., 1975

22. S. Forrest, F. Hofmeyr, A. Somayaji, T. A. Longstaff, “A Sense of Self for Unix Processes”, Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, Los Alamitos, CA, 1996

24. D. Dasgupta (Ed.) Artificial Immune Systems and Their Applications, Springer, 1998

25. D. Dasgupta and F. Gonzalez. An Immunity-Based Technique to Characterize Intrusions in Computer Networks. To appear in the journal IEEE Transactions on Evolutionary Computation, Vol. 6, No. 3, June 2002